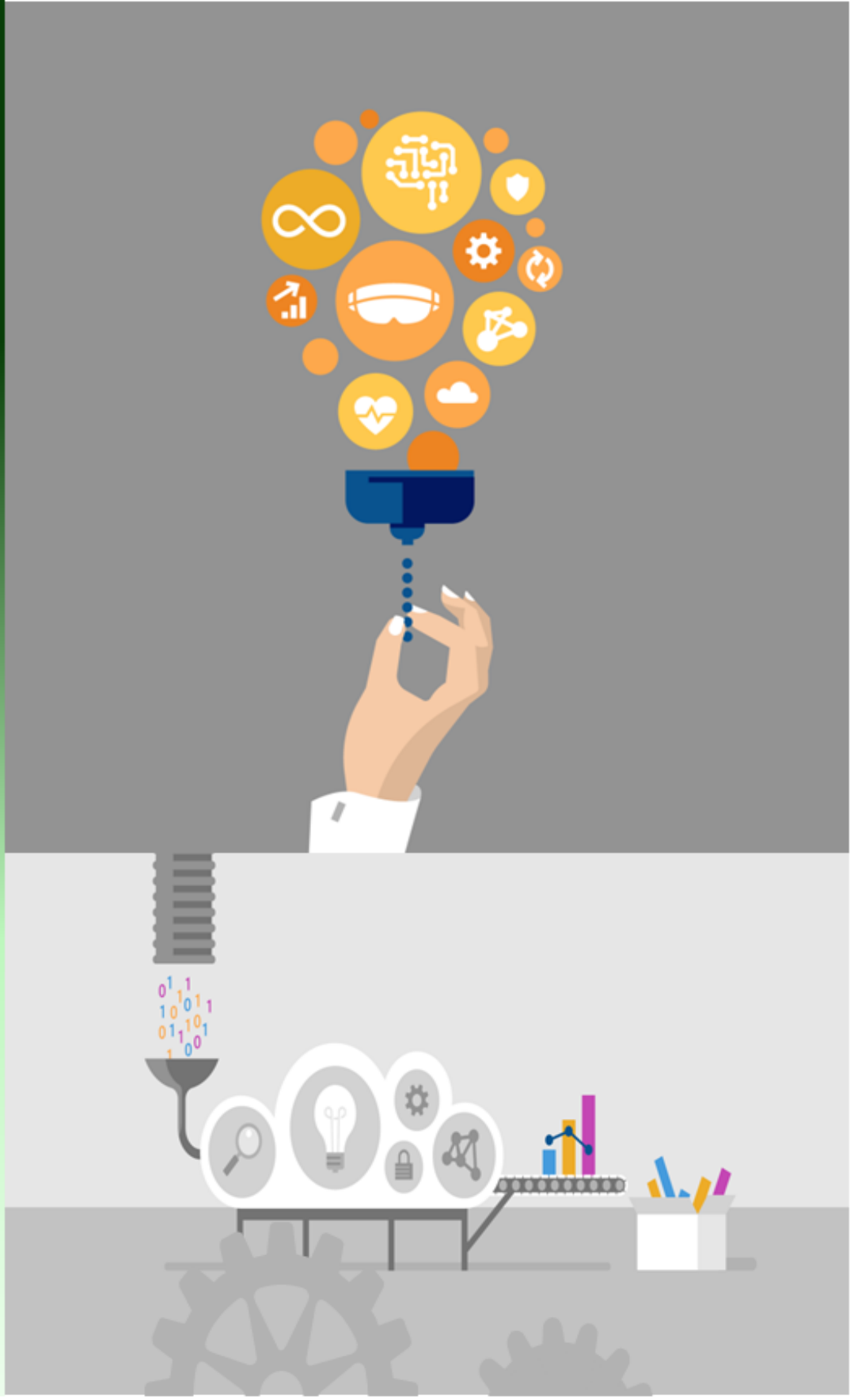

CLOUD FIRST POLICY - PRIVACY and LEGAL CHECKLIST

premier

Office Of The Premier
PROVINCE OF KWAZULU-NATAL

premier

Office Of The Premier
PROVINCE OF KWAZULU-NATAL

CLOUD FIRST PRIVACY and LEGAL CHECKLIST

Version 1.0.0

Date: 28 February 2020

Accreditation

This document is platformed, with credit, on the DPSA Cloud first policy that is awaiting ratification. It contains the basis of the required information from the policy with upliftment to address pertinent financial decision making pertinent to cloud within the province of Kwazulu Natal.

Document Version Control

Date	Author	Version
23 January 2020	KZN OTP ICT DEPT	Version 0.0.1
28 February 2020	KZN OTP ICT DEPT	Version 1.0.0

Approvals

The Cloud First Business Case Template is approved by the Director General of the Province.

Name	Signature	Date

Review Period

This template will be reviewed annually or subsequent to any significant issue arising that has not been considered

Name	Signature	Date

Contact Information

For more information on this policy or to inquire about a variation that is not covered, pls contact the KZN Office of The Premier ICT Governance Department.

TABLE OF CONTENTS

Definitions/Glossary

DPSA	Department of Public Service and Administration
GCIO	Government Chief Information Office
GITOC	Government Information Technology Officer Council
SITA	State Information Technology Agency
PSA	Public Service Act
ICT	Information and Communications Technology
SSA	State Security Agency
ISO	International Standards Organisation
ISACA	Information Systems Audit and Control Association
NIST	The National Institute of Standards and Technology
CSP	Cloud Service Provider
HIPAA	Health Insurance Portability and Accountability Act (USA)
GDPR	General Data Protection Regulation (European Union)
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
ISO/IEC27001/ ISO17799	Information security management Standard

Legislative

Public Service Act 30 of 2007
Public Service Regulations of 2001 as amended 16 July 2004
Public Administration Management Act of 2014
Promotion of Access to Information Act, No 2 of 2000
State Information Technology Agency Act no 88 of 1998
Intelligence Services Act 65 of 2002 - SSA
National Archives of South Africa Act 43 of 1996
The Protection of Personal Information Act no 4 of 2013(POPI)

Privacy Checklist

Privacy checkpoints template for a cloud solution[1]

This privacy checklist contains a non-exhaustive list of issues related to privacy and information security that a department should investigate when considering cloud based services to ensure that the contract they agree with cloud service providers adequately addresses the applicable privacy obligations.

Departments are advised to conduct a risk-based analysis of their information, including a Privacy Impact Assessment, to determine the most appropriate ICT environment to deploy to support the classification of their information and business requirements.

Where a department cannot adequately address their privacy obligations it will not be appropriate to transfer that information into a public cloud environment.

Summary of Privacy Checkpoints

1. Has your department established a policy or procedure for deciding when it will be appropriate to use cloud computing services? Does the policy or procedure address the following? a) will the proposal involve the storage or processing of personal information? b) if so, is an assessment of the ability of a cloud solution to provide adequate protection to the personal information required? c) if personal information is involved, what extra measures might be required? d) what type of cloud service provider will be appropriate? (e.g. private, public or hybrid) Reference: ***POPI & PAIA***	
2. Has your department decided what it will use cloud service infrastructure for? a) just storing b) just processing c) both storing and processing	

[1] Adopted from Privacy and Cloud Computing for Australian Government 2013

3. Has your department developed a contract with the cloud service provider that is consistent of the ***POPI & PAIA***? How will your department ensure that the contract's requirements are being met?	
4. Has your department considered what specific terms should be included in the contract to complement the general requirement under POPI Act? Some specific matters that could be addressed in the contract include requirements relating to: a) data breach notification b) the location of information c) access to information by department staff and individuals d) audits	
5. If personal information is to be disclosed or used to a cloud service provider, has your department determined how that disclosure will be authorised? a) express permission from individuals b) individuals are notified in privacy notice/terms and conditions c) by legislative provisions	
6. If you are intending to use an offshore cloud service provider, do you know where their head office is located? What are the privacy implications?	
7. Does your department know where the data will be stored; keeping in mind the possibility it may be across different countries or continents? What are the Privacy implications?	
8. Keeping in mind privacy law reform, has your department determined that there is data protection or privacy legislation in place in relevant foreign jurisdictions that, at a minimum, meets the requirements in the *POPI Act*? Is the relevant law enforceable?	
9. Has your department determined how the personal information will be kept separate from other organisations' data housed in the cloud service provider's infrastructure?	

10. Has your department determined how employees of the cloud service provider will be prevented from unauthorised access to the data? Has your department decided how it will control a cloud service provider passing personal information onto unauthorised third party organisations or using it for purposes other than those it was originally collected for?	
11. Has your department determined how it will monitor the cloud service provider's use and management of the department's information?	
12. Has your department determined the controls (for example, encryption) that will be in place to ensure the security of personal information as it travels between here and possible overseas cloud data storage location?	
13. If a South African citizen requests access or alteration to their personal information, has your department put in place appropriate controls so that all copies can be retrieved and amended easily? Has your department put in place arrangements to ensure that where an individual requests an amendment to their personal information and this request is not agreed to, it will be possible to attach a statement provided by the individual regarding the requested amendment to the record?	
14. Has your department ensured that the cloud service provider will hold the personal information only as long as your department needs it? Has your department specified how the cloud service provider will manage their backup regime? Has your department specified how personal information that is no longer needed is to be destroyed or de-identified?	
15. Has your department determined what happens at the conclusion of the contract with the cloud service provider? Will information be able to be retrieved or destroyed (including all backups where appropriate) in compliance with the POPI Act and associated legislation?	

Legal checklist template for a cloud Solution2

The following checklist identifies the typical legal issues departments should consider when signing any agreement with the cloud service provider.

Departments should always ensure that they have properly reviewed, and obtained all necessary specific legal advice on, any agreement they wish to enter.

Protection of information

- ☐ privacy
- ☐ security
- ☐ confidentiality
- ☐ records management requirements
- ☐ audit
- ☐ compensation for data loss/misuse
- ☐ subcontractors

Liability

- ☐ limitations on liability
- ☐ indemnity

Performance management

- ☐ service levels
- ☐ response times
- ☐ flexibility of service
- ☐ business continuity and disaster recovery

Ending the arrangement

- ☐ termination for convenience and early termination fees termination for
- ☐ default provider's right to terminate
- ☐ legal advice on termination
- ☐ disengagement/transition of services
- ☐ intellectual property ownership
- ☐

Dispute resolution

- ☐ choice of law

Other legal issues

- ☐ introduction of harmful code
- ☐ change of control and assignment/innovation
- ☐ change of terms at discretion of the
- ☐ provider application of foreign laws and transborder data transfer

further issues:

Promotion of access to information act 2 of 2000

- ☐ obligations intellectual property
- ☐ ownership publicity by the provider in respect of agreement
- ☐ use of Department branding and
- ☐ logos by the provider responsibility for end-users export controls
- ☐ requirement to take updates

Managing the agreement

- ☐ ensure that agreement terms are appropriate and reasonable
- ☐ understand the terms of the agreement
- ☐ and keep a copy handy
- ☐ enforce the service level arrangements be prepared to audit the provider within reasonable limits
- ☐ maintain a good relationship with the provider
- ☐ if things go wrong, be aware of contractual rights and obligations
- ☐ seek legal advice if difficult issues arise

[2] Adopted from Negotiating the cloud – legal issues in cloud computing agreements. Australian Government, 2012

Cloud Service Provider Compliance and Accreditations

Global Cloud Accreditations

The following global cloud accreditations should be downloaded and submitted apart of the project as proof of compliance to the Cloud First Policy :

- ☐ CIS Benchmark
- ☐ CSA-STAR attestation
- ☐ CSA-STAR certification
- ☐ CSA-STAR self-assessment
- ☐ ISO 20000-1:2011
- ☐ ISO 22301
- ☐ ISO 27001
- ☐ ISO 27017
- ☐ ISO 27018
- ☐ ISO 27701
- ☐ ISO 9001
- ☐ SOC
- ☐ WCAG

Industry Specific Cloud Accreditations

The Province of KwaZulu Natal has a vision to be a gateway to the world. As responsible global citizens, the Cloud Service Provider should attest to compliance in these industry specific accreditations to demonstrate capability of both local and global relevance.

☐ 23 NYCRR Part 500	☐ HITRUST
☐ AFM + DNB (Netherlands)	☐ KNF (Poland)
☐ APRA (Australia)	☐ MARS-E
☐ AMF and ACPR (France)	☐ MAS + ABS (Singapore)
☐ CDSA	☐ MPAA
☐ CFTC 1.31 (US)	☐ NBB + FSMA (Belgium)
☐ DPP (UK)	☐ NEN-7510 (Netherlands)
☐ EBA (EU)	☐ NERC
☐ FACT (UK)	☐ NHS IG Toolkit (UK)
☐ FCA (UK)	☐ OSFI (Canada)
☐ FDA CFR Title 21 Part 11	☐ PCI DSS
☐ FERPA	☐ RBI + IRDAI (India)
☐ FFIEC (US)	☐ SEC 17a-4
☐ FINMA (Switzerland)	☐ SEC Regulation SCI
☐ FINRA 4511	☐ Shared assessments

☐ FISC (Japan) ☐ FSA (Denmark) ☐ GLBA ☐ GxP ☐ HDS (France) ☐ HIPAA / HITECH	☐ SOX ☐ TISAX (Germany) ☐ TruSight

ISO/IEC 19086-1 Standard (Optional but to be read)

The ISO/IEC 19086-1 is the first of a new four-part international standard that establishes both a framework and terminology for cloud service level agreements (SLAs). It offers a unified set of considerations for organizations considering cloud adoption, and common terminology so they can more easily compare cloud services and providers to ultimately establish an SLA.
https://www.iso.org/standard/67545.html

The goal was to create a simpler document that organizations considering a move to the cloud, as well as cloud service providers, could use to create a cloud service agreement. This initiative has reduced complexity to a two-page Cloud Services Due Diligence Checklist that can apply to all organizations and cloud service providers.

An abbreviation of the checklist is available here or from the Office of The Premier.